

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

<p>LYNETTE ARMSTRONG, on behalf of herself and all others similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p>TANDYM GROUP, LLC,</p> <p style="text-align: center;">Defendant.</p>	<p>Case No.</p> <p>JURY TRIAL DEMANDED</p> <p>CLASS ACTION</p>
---	--

CLASS ACTION COMPLAINT

Plaintiff Lynette Armstrong, individually and on behalf of all similarly situated persons, alleges the following against Tandym Group, LLC, ("Tandym" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Tandym for its failure to properly secure and safeguard Plaintiff's and other similarly situated Tandym employees' sensitive information, including but not limited to names and Social Security numbers ("personally identifiable information" or "PII").
2. Defendant is an employee staffing company.
3. Upon information and belief, former and current employees of Defendant are required to entrust Defendant, directly or indirectly, with sensitive, non-public PII, without which

Defendant could not perform its regular business activities. Defendant retains this information for at least many years and even after the employee-employer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. In or around May 30, 2023, Defendant became aware of suspicious activity related to a Tandym employee's email account. In response, Defendant launched an investigation through which it determined that "an unauthorized individual accessed an employee Microsoft Outlook account as well as our iSolved system on May 18, 2023."¹ As a result of its investigation, Defendant concluded that Plaintiff's and Class Members' PII was compromised in the Data Breach.²

6. According to Tandym's letter, sent to Plaintiff and Class Members on behalf of Defendant (the "Notice Letter"), the compromised PII included individuals' name and Social Security number.³

7. Defendant failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect employees' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

¹ Notice of Data Breach attached hereto as **Exhibit A**.

² *Id.*

³ *Id.*

8. Hackers targeted and obtained Plaintiff's and the Class Members' PII with the intent to use the information fraudulently.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to

access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

13. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

15. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class.

PARTIES

16. Plaintiff Lynette Armstrong, is, and at all times mentioned herein was, an individual citizen of Georgia and is a former employee of Defendant.

17. Defendant Tandym Group, LLC, is a New York limited liability company corporation with its principal place of business located in New York, New York.

JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of New York and have different citizenship from Tandym, including Plaintiff, a citizen of Georgia. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

19. This Court has jurisdiction over Tandym because Tandym operates in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Tandym has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendant's Business

21. Defendant is staffing and recruiting company based in New York. Founded in 1985, Tandym offers direct hire recruitment, contract/consulting, and contract-to-hire solutions for companies of all sizes.⁴

22. Plaintiff and Class Members are current and former employees of Defendant's.

23. As a condition of receiving employment, Tandym requires that its employees, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

24. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

25. Upon information and belief, Defendant made promises and representations to its employees, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining employment from Defendant, employee PII would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

26. Plaintiff and Class Members provided their PII to Defendant, directly or indirectly, with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from

⁴ <https://www.linkedin.com/company/tandymgroup/about/> (last accessed April 22, 2024).

unauthorized access.

27. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

28. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's PII safe and confidential.

29. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

30. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

32. On or about April 5, 2024, Defendant, began sending Plaintiff and other Data Breach victims a Notice of Data Beach letter (the "Notice Letter"), informing them that:

What Happened? On May 30, 2023, Tandym became aware of suspicious activity related to a Tandym employee's email account. We immediately launched an

investigation into the nature and scope of the incident with the assistance of industry-leading cybersecurity specialists. The investigation determined that an unauthorized individual accessed an employee Microsoft Outlook account as well as our iSolved system on May 18, 2023. On or around January 12, 2024, we completed our review of the information that was stored in the impacted systems. Tandem is notifying you out of an abundance of caution.

What Information Was Involved? The review identified the following types of sensitive information relating to you were present: Social Security number and your name.⁵

33. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

34. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

35. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

36. The attacker accessed and acquired files Defendant retained containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff’s and Class Members’ PII was accessed and stolen in the

⁵ Exhibit A.

Data Breach.

37. Upon information and belief, the PII of Plaintiff, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

38. Defendant could have prevented this Data Breach by, among other things, properly encrypting PII being shared with its vendors or otherwise ensuring that such PII was protected while in transit or accessible.

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

40. The unencrypted PII of Class Members already has and will continue to be for sale to identity thieves on the dark web or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

41. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁶

42. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

⁶ How to Protect Your Networks from RANSOMWARE, at 3, available at: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last accessed Apr. 22, 2024).

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁷

43. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

⁷ *Id.* at 3-4.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].⁸

44. Given that Defendant was storing and sharing the PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of thousands of current and former employees of Defendant, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Plaintiff's and the Class's PII

46. As a condition to obtain employment from Tandem, Plaintiff and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Defendant.

47. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to offer employment to Plaintiff and Class Members.

48. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

49. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

⁸ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last accessed Jan. 24, 2024).

50. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

51. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

52. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk Because Companies In Possession Of PII Are Particularly Susceptible To Cyber Attacks

53. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting companies that collect and store PII, like Defendant, preceding the date of the breach.

54. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

55. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁹

56. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive

⁹ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

records (9,700,238) in 2020.¹⁰

57. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹¹

58. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

59. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

61. At all relevant times, Defendant knew, or reasonably should have known, of the

¹⁰ *Id.*

¹¹ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Jan. 24, 2024).

importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

62. Additionally, as companies became more dependent on computer systems to run their business,¹² *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹³

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

64. In the Notice Letter, Defendant offers to cover credit monitoring services for a period of 12 months. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity and/or credit monitoring services.

65. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from

¹² <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last accessed Jan. 24, 2024).

¹³ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022> (last accessed Jan. 24, 2024).

Defendant's computer systems.

66. Defendant's offer of credit and identity monitoring establishes that there is in fact an imminent risk of misuse of Plaintiff's and the Class Members' PII that is certainly impending.

67. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

68. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security number—fraudulent use of that information and damage to victims may continue indefinitely.

69. As a company in possession of its current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁴ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

¹⁴ 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number.”¹⁵

71. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁶

72. For example, PII can be sold at a price ranging from \$40 to \$200.¹⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁸

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—bank account and routing numbers, social security numbers and passport information.

74. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”¹⁹

75. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

Tandym Failed to Comply with FTC Guidelines

¹⁵ *Id.*

¹⁶ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Apr. 22, 2024).

¹⁷ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Apr. 22, 2024).

¹⁸ *In the Dark*, VPNOview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Apr. 22, 2024).

¹⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Apr. 22, 2024).

76. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g.,* *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

77. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

78. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. These FTC enforcement actions include actions against insurance companies, like Defendant.

81. As evidenced by the Data Breach, Tandym failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Tandym's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

82. Tandym was at all times fully aware of its obligation to protect the PII of its employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Tandym Failed to Comply with Industry Standards

83. As noted above, experts studying cybersecurity routinely identify companies like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

84. Some industry best practices that should be implemented by companies dealing with sensitive PII, like Tandym, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

85. Other best cybersecurity practices that are standard include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

86. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Tandym Breached its Duty to Safeguard Plaintiff's and Class Members' PII

88. In addition to its obligations under federal and state laws, Tandym owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Tandym owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members.

89. Tandym breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Tandym's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect employees' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- e. Failing to sufficiently train its employees and vendors regarding the proper handling of its employees' PII;
- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- g. Failing to adhere to the industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

90. Tandym negligently, unlawfully, and recklessly failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

91. Had Tandym remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its

information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

Common Injuries & Damages

92. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

93. As a result of Defendant's ineffective and inadequate data security practices and the Data Breach, Plaintiff's and Class Members' PII has already been sold or otherwise posted for sale on the darkweb for cybercriminals to access and fraudulently misuse the PII.

94. This actual misuse of Plaintiff's and Class Members' PII constitutes both a present injury and a substantial imminent risk of harm in the future.

95. Plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress.

The Data Breach Increases Victims' Risk Of Identity Theft

96. Not only has Plaintiff's and Class Members' PII already sold and posted on the darkweb, but Plaintiff and Class Members are at a heightened risk of identity theft for years to

come.

97. The unencrypted PII of Class Members already has been sold on the darkweb and will continue to end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

98. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

99. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

100. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

101. One such example of criminals piecing together bits and pieces of compromised

PII for profit is the development of “Fullz” packages.²⁰

102. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

103. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

104. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver’s license numbers) of Plaintiff and the other Class Members.

105. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

106. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to

²⁰ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/>. (Last accessed Apr. 22, 2024)

crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

107. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

108. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter instructs,²¹ "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

109. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

110. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."²²

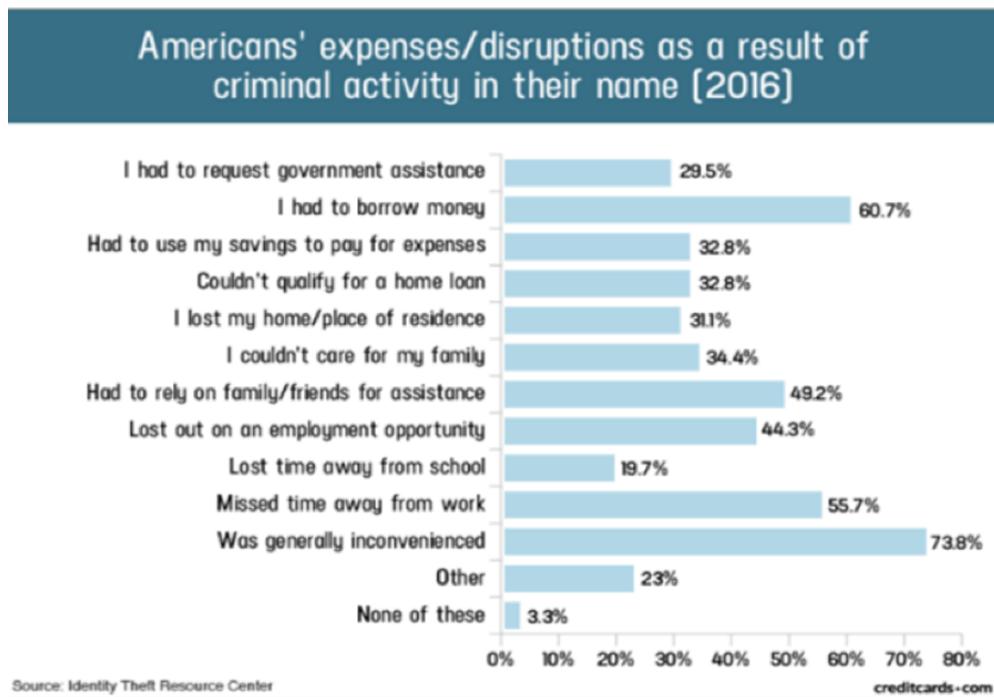
111. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data

²¹ Notice Letter.

²² See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²³

112. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.²⁴



113. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁵

²³ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last accessed Apr. 22, 2024).

²⁴ Credit Card and ID Theft Statistics” by Jason Steele, 10/24/2017, at: <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Sep 13, 2022).

²⁵ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the

Diminution Value Of PII

114. PII is a valuable property right.²⁶ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

115. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.²⁷

116. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{28,29}

117. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁰

118. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³¹

119. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by

Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last accessed Apr. 22, 2024) ("GAO Report").

²⁶ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

²⁷ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed Apr. 22, 2024).

²⁸ <https://datacoup.com/> (last accessed Apr. 22, 2024).

²⁹ <https://worlddataexchange.com/about> (last accessed Apr. 22, 2024).

³⁰ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last accessed Apr. 22, 2024).

³¹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed Apr. 22, 2024).

its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

120. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

121. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

122. The fraudulent activity resulting from the Data Breach has already occurred and will likely continue for years.

123. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

124. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to thousands of individuals’ detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

125. The injuries to Plaintiff and Class Members were directly and proximately caused

by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

126. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

127. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

128. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

129. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of The Benefit Of The Bargain

130. Furthermore, Defendant's poor data security deprived Plaintiff and Class

Members of the benefit of their bargain. When agreeing to employment with Defendant, Plaintiff and other Class Members understood and expected that they were, in part, providing their services to Defendant in exchange for payment and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received payment and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Experience

131. Plaintiff Lynette Armstrong was an employee of Tandym.

132. As a condition of receiving employment with Tandym, she was required to provide her PII, directly or indirectly, to Defendant, including her name, date of birth, Social Security number, and other highly sensitive personal information.

133. At the time of the Data Breach—in or around May, 2023—Defendant retained Plaintiff's PII in its system.

134. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

135. Plaintiff Lynette Armstrong received the Notice Letter, by email, from Defendant, in or about April, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

136. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for

credit monitoring services, freezing her accounts. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

137. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

138. Plaintiff was also notified of actual misuse of her PII in that a credit card was issued with a \$15,000 limit to her name, which she did not authorize.

139. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

140. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

141. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and the actual misuse resulting from her PII, especially her Social Security number, being placed in the

hands of criminals.

142. Because their personally identifying and financial information, including but not limited to their Social Security numbers, has been accessed by criminals, Plaintiff and the Class have suffered concrete and ongoing injuries.

143. According to experts, one out of four data breach notification recipients become a victim of identity fraud.³²

144. Plaintiff Lynette Armstrong has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

145. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

146. Specifically, Plaintiff proposes the following Nationwide Class, subject to amendment as appropriate:

Nationwide Class:

All persons Defendant has identified as being among those individuals impacted by the Data Breach in or around May, 2023, including all who were sent a notice of the Data Breach (the "Class").

147. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

³² *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, THREATPOST.COM (Feb. 21, 2013), <https://bit.ly/3zB8Uwv> (last accessed Apr. 22, 2024)

148. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

149. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

150. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time it is likely hundreds, if not thousands of individuals had their PII compromised in this Data Breach, given the Defendant operates widely throughout the United States. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

151. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Tandym engaged in the conduct alleged herein;
- b. Whether Tandym's conduct violated the FTCA;
- c. When Tandym learned of the Data Breach;
- d. Whether Tandym's response to the Data Breach was adequate;
- e. Whether Tandym unlawfully lost or disclosed Plaintiff's and Class Members' PII;
- f. Whether Tandym failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
- g. Whether Tandym's data security systems prior to and during the Data Breach

complied with applicable data security laws and regulations;

- h. Whether Tandym's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether Tandym owed a duty to Class Members to safeguard their PII;
- j. Whether Tandym breached its duty to Class Members to safeguard their PII;
- k. Whether hackers obtained Class Members' PII via the Data Breach;
- l. Whether Tandym had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether Tandym breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- n. Whether Tandym knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of Tandym's misconduct;
- p. Whether Tandym's conduct was negligent or reckless;
- q. Whether Tandym was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

152. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Tandym. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

153. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

154. Predominance. Tandym has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Tandym's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

155. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Tandym. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

156. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Tandym has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

157. Finally, all members of the proposed Class are readily ascertainable. Tandym has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Tandym.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

158. Plaintiff restates and realleges paragraphs 1-157 of this Complaint and incorporates them by reference herein.

159. Defendant owed a duty to reasonably safeguard data that Plaintiff and the Class entrusted to it in the scope of their employment.

160. Defendant requires its employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of receiving employment.

161. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting employment with Defendant, which solicitations and services affect commerce.

162. Plaintiff and Class Members entrusted Defendant with their PII, directly or

indirectly, with the understanding that Defendant would safeguard their information.

163. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

164. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

165. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

166. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

167. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant, Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment with Defendant.

168. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is

bound by industry standards to protect confidential PII.

169. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiff or the Class.

170. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees’ PII it was no longer required to retain pursuant to regulations.

171. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

172. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant’s possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

173. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members’ PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to audit, monitor, or ensure the integrity of its vendor’s data security practices;
- d. Allowing unauthorized access to Class Members’ PII;
- e. Failing to detect in a timely manner that Class Members’ PII had been

compromised;

- f. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

174. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

175. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

176. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

177. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

178. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

179. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

180. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

181. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

182. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

183. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

184. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

185. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See Restatement (Second) of Torts § 302B.* Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

186. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost

and disclosed to unauthorized third persons as a result of the Data Breach.

187. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

188. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

189. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

190. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

191. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

192. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

193. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

194. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf Of Plaintiff And the Class)

195. Plaintiff restates and realleges paragraphs 1-157 of this Complaint and incorporates them by reference herein.

196. Plaintiff and the Class entrusted their PII to Defendant as a condition of obtaining employment and receiving services from Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. These implied contracts may be composed, in part, of the written policies posted on Defendant's website, including its Privacy Policy and Terms of Use.

197. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not

take unjustified risks when storing the PII.

198. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

199. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements such as bank account and routing numbers, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

200. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

201. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised because of the Data Breach.

202. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the

compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

203. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
Breach Of Fiduciary Duty
(On Behalf Of Plaintiff And the Class)

204. Plaintiff restates and realleges paragraphs 1-157 of this Complaint and incorporates them by reference herein.

205. In providing their PII, directly or indirectly, to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and class members to safeguard and keep confidential that PII.

206. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's and Class Members' personal information as detailed in its Privacy Policy.

207. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its employees, including Plaintiff and Class members, for the safeguarding of Plaintiff and Class member's PII.

208. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members

upon matters within the scope of its relationship with Defendants' employees, in particular, to keep secure the PII of its employees.

209. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's PII.

210. Defendant breached its fiduciary duties to Plaintiff and class members by otherwise failing to safeguard Plaintiff's and Class members' PII.

211. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

212. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Unjust Enrichment / Quasi Contract
(On Behalf Of Plaintiff And the Class)

213. Plaintiff restates and realleges paragraphs 1-157 of this Complaint and incorporates them by reference herein.

214. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiff and Class

Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

215. Defendant appreciated that Plaintiff and Class Members were conferring a benefit upon it and accepted that monetary benefit.

216. Acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

217. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

218. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

219. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

220. Plaintiff and Class Members have no adequate remedy at law.

221. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

222. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

223. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;
- D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 - iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to

conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

- vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. Requiring Defendant to conduct regular database scanning and securing checks;
- xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security

personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class,

and to report any deficiencies with compliance of the Court's final judgment.

- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
- G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- H. For an award of punitive damages, as allowable by law;
- I. Pre- and post-judgment interest on any amounts awarded; and
- J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: April 24, 2024

Respectfully submitted,

SHAMIS & GENTILE P.A.

/s/Andrew J. Shamis

Andrew J. Shamis, Esq.

/s/ Leanna A Loginov

Leanna A. Loginov, Esq.

14 NE 1st Ave., Suite 705

Miami, Florida 33132

Tel: (305) 479-2299

ashamis@shamisgentile.com

lloginov@shamisgentile.com

*Attorneys for Plaintiff and
the Proposed Class*